Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BRITISH TELECOMMUNICATIONS PLC) and BT AMERICAS, INC., *Plaintiffs*, v. PALO ALTO NETWORKS, INC. *Defendant*.	C.A. No. 22-01538-CJB

DEFENDANT'S ANSWERING CLAIM CONSTRUCTION BRIEF

Dated: April 24, 2024

OF COUNSEL:

Adrian C. Percer (admitted *pro hac vice*)
Gregg T. Stephenson (admitted *pro hac vice*)
Weil, Gotshal & Manges LLP
201 Redwood Shores Parkway
Redwood Shores, CA 94065
Telephone: (650) 802-3000
adrian.percer@weil.com
gregg.stephenson@weil.com

Anish R. Desai (admitted *pro hac vice*)
Ian Moore (admitted *pro hac vice*)
Tom Yu (admitted *pro hac vice*)
Weil, Gotshal & Manges LLP
767 Fifth Avenue
New York, NY 10153
Telephone: (212) 310-8000
anish.desai@weil.com
ian.moore@weil.com
tom.yu@weil.com

Priyata Y. Patel (admitted *pro hac vice*)
Weil, Gotshal & Manges LLP
2001 M Street, NW Suite #600
Washington, D.C. 20036
Telephone: (202) 682-7000
priyata.patel@weil.com

Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
FARNAN LLP
919 North Market St., 12th Floor
Wilmington, DE 19801
Tel: (302) 777-0300
Fax: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Attorneys for Defendant Palo Alto Networks, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF EXHIBITS

EXHIBIT	DESCRIPTION
Exhibit 1	Declaration of Dr. John Villasenor in Support of Defendant Palo Alto Network, Inc.'s Answering Claim Construction Brief
Exhibit 2	Stalling, "Cryptography and Network Security," 5th Edition (2011)
Exhibit 3	Saiedian, Hossein, "Computer Security: Principles and Practice," (2014)
Exhibit 4	Strom, D., "The Packet Filter: A Basic Network Security Tool," (Sept. 25, 2000)
Exhibit 5	Chapman, D., "Network (In)Security Through IP Packet Filtering"
Exhibit 6	McGraw-Hill Dictionary, 5th Edition, definition of "filter"
Exhibit 7	Plaintiffs' Preliminary Infringement Contentions
Exhibit 8	Merriam Webster's Dictionary, 10th Edition, definition of "empirical"

Defendant Palo Alto Networks, Inc. ("PAN") hereby submits its Answering Claim Construction Brief.

I. PRELIMINARY STATEMENT

U.S. Patent No. 7,159,237 (the "'237 Patent") was filed Jan. 19, 2001 and expired May 11, 2023. The '237 Patent claims a method of "filtering" data followed by analysis of "post-filtering residue" wherein "identified events are transmitted to a human analyst for problem resolution." *See generally* '237 Patent, D.I. 122, Ex. A.

II. DISPUTED CONSTRUCTIONS

A. The "Filtering" Terms (Nos. 1-3)

The key dispute for the filtering terms is whether "filtering" as recited in Term Nos. 1-3 includes positive filtering, negative filtering, ***or*** both as PAN contends, or instead requires ***both*** positive ***and*** negative filtering as BT contends. Understanding the various types of filtering and how they function is foundational to that dispute. As explained below, PAN's position is consistent with the plain and ordinary meaning of "filtering," as well as how filtering is claimed and described in the '237 Patent. In contrast, BT's position conflicts with the claim language and the specification, and is also contrary to how the term "filtering" is used in the prior art.

1. Technical Background on Filtering

In the context of "network security," a person of skill in the art ("POSA") would have understood "filtering" to mean comparing data with a known criterion, and, if the data matches that criterion, taking a specified action. *See* Ex. 1 (Dr. John Villasenor Decl.) at ¶¶ 26-31. A POSA would further have understood such specified actions may include: (1) blocking/discarding the data, and (2) selecting/forwarding the data. *Id.* at ¶¶ 26-27 (citing '237 Patent at 8:45-59).

This is exactly how the '237 Patent describes filtering—a negative filter discards data that matches a criterion and/or a positive filter selects data that matches another criterion. '237 Patent at 8:45-59. Specifically, the '237 Patent explains that, in an exemplary embodiment, "the data is first filtered by negative filtering . . . , which ***discards uninteresting information***," meaning that the negative filter blocks information because that information matches a criterion (and is therefore "uninteresting"). *Id.* at 8:45-47.[1] The data is then filtered "by positive filtering…, which ***selects possibly interesting information and forwards it*** to communications and resource coordinator," meaning that the positive filter selects and forwards information because that information matches another criterion (and is therefore "possibly interesting"). *Id.* at 8:53-55. The patent expressly contemplates that not all data will match a filter criterion. That is, some data may be neither blocked nor selected. The '237 Patent calls this "residue" data, which is data "neither discarded by negative filtering [] nor selected out as interesting by positive filtering." *Id.* at 8:55-57.

The '237 Patent acknowledges that this understanding of positive and negative "filtering" was "well-known to those skilled in the art." *Id.* at 8:59. Indeed, it is consistent with prior art definitions of filtering. For example, a September 2000 reference provides that a "filtering device compares the values of these fields to ***rules that have been defined***[, *i.e.*, criteria], and based upon the values and the rules the packet[,] is ***either*** passed ***or*** discarded." *See* Ex. 1 at ¶ 28 (citing Ex. 4 at 1-3); *see also* Ex. 2 at 20 ("A firewall may act as a packet filter. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria."); Ex. 3 at 6 ("Positive [] filter: Allow [] packets that meet a criteria" and "[] (negative) filter: [] (reject) packets that meet a criteria") Ex. 5 at 65 ("filtering

[1] Emphasis added unless otherwise stated.

rules are expressed as a table of ***conditions and actions***"); Ex. 6 at 754 (defining filter as "A device or program that separates data or signals in accordance with ***specified criteria***").

BT's usage of the terms "positive filter," "negative filter," "select," and "discard" in its preliminary infringement contentions are inconsistent with how those terms are used in the '237 Patent and in the prior art. ***First***, BT's contentions state:

> The following representative excerpt describes the Security Policy actions, which includes the ***"deny" action (positive filtering)***. The "deny" action ***selects*** the filtered status data and takes the default Deny Action defined for the related application.

Ex. 7 (Plaintiff's Preliminary Infringement Contentions) at 32. Here, BT incorrectly asserts that positive filtering denies (*i.e.*, discards) incoming data. As explained above, the '237 Patent is clear that positive filtering means selecting data and negative filtering means discarding data. '237 Patent at 8:45-50.

Additionally, BT uses the term "select" to refer to data *matching* the filter criterion. Ex. 7 at 25. But in the '237 Patent, "select" refers to the *action* taken by a positive filter *after* the data matches the filter criterion. *Id.* at 8:45-50; Claims 1, 18, 26.

BT's contentions further state:

> PAN negatively filters the status data at least through exception lists. As explained by PAN below, 'threat exception[s] for specific IP addresses' can be added, which 'will add a threat exception with the IP addresses added as a filter on the threat exception.' This ***negatively filters the IP address status data by discarding IP addresses that match this filter*** so that it is ignored.

Ex. 7 at 36. Here, BT correctly uses the word "match" to refer to data meeting a filter criterion, and also correctly identifies a negative filter as a filter that discards incoming data upon a match. But this highlights BT's inconsistent usage of positive and negative filtering between these two examples.

BT's contentions also state that:

> Security profile ***filter rules that are configured to block data based on a match represent positive filtering***, and ***security policy rules that allow data represent negative filtering***.

Ex. 7 at 39. Here, BT correctly uses the term "match" again, but incorrectly asserts that a positive filter blocks/discards while a negative filter allows/selects.

BT's confusing and inconsistent contentions highlight the need for claim construction of the filtering terms.

2. Term No. 1: "post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering"

Term	Claim Nos.	BT's Proposed Construction	PAN's Proposed Construction
post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering	Claims 1, 18, 26	Status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering	Plain and ordinary meaning, which is "data that does not match any filter (*i.e.*, discarding (negative) filter and/or selecting (positive) filter)"

The parties dispute whether post-filtering residue must undergo ***both*** positive ***and*** negative filtering. As explained below, (1) the plain language does not require both positive and negative filtering, (2) the dependent claims support that the independent claims do not require both negative filtering and positive filtering, and (3) the specification includes embodiments that do not require both positive and negative filtering. Therefore, the Court should adopt the plain and ordinary meaning of "post-filtering residue," which is "data that does not match any filter (*i.e.*, discarding (negative) filter and/or selecting (positive) filter)."

a) The Claim Language Does Not Require Both Positive Filtering And Negative Filtering

In the patentee's own words, the "term 'post-filtering residue' is clearly defined, ***in the claim language itself***, as data that is neither discarded nor selected by filtering." '237 Patent File

History, D.I. 122, Ex. C ("'237 File History"), JA-0000121 (Applicant's Arguments and Remarks at 8 (Feb. 3, 2006)). The relevant claim language broadly covers residue that undergoes any type of filtering—positive and/or negative filtering. Claim 1, for example, recites "analyzing status data . . . wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." '237 Patent at Claim 1. This language requires only that analyzing status data (1) "includes filtering," and (2) a further analysis of any status data that was "neither discarded nor selected by filtering." *Id.* at Claims 1, 18, 26. The claim language does not require positive ***and*** negative filtering. It simply recites "filtering"—any type of filtering. Contrary to BT's position, this means positive filtering, negative filtering, or both. And any data that was neither discarded nor selected (*i.e.*, post-filtering residue) undergoes further analysis.

Three hypotheticals are helpful in demonstrating the plain language of the claims:

- **Hypothetical #1:** The filtering system has at least one positive filter. Incoming data is compared to the positive filter(s). If there is a match, then the data is selected by filtering and there is no residue. If there is no match on at least one positive filter, then that data is "post-filtering residue" because it was neither selected nor discarded by the filtering system.
- **Hypothetical #2:** The filtering system has at least one negative filter. Incoming data is compared to the negative filter(s). If there is a match, then the data is discarded by filtering and there is no residue. If there is no match on at least one negative filter, then that data is "post-filtering residue" because it was neither selected nor discarded by the filtering system.

- **Hypothetical #3:** The filtering system has both positive and negative filters. Incoming data is compared to the positive filter(s). If there is a match, then the data is selected by filtering. The data is also compared to the negative filter(s). If there is a match, then the data is discarded by filtering. Data that does not match any positive filter and any negative filter is "post-filtering residue" because it was neither selected nor discarded by the filtering system.

In all three hypotheticals above, there can be leftover data (*i.e.*, post-filtering residue) that does not match on a filtering criterion, and is therefore data that was neither discarded nor selected by filtering.

Nonetheless, despite the plain language of the claims, BT contends that "the terms '***neither***' and '***nor***' within the claim language require that the data must have gone through both negative and positive filtering." Pl. Op. Brief at 8.[2] Yet the terms "neither" and "nor" precede and modify the words "discarded" and "selected," respectively. '237 Patent at Claims 1, 18, 26. They do not modify "positive filtering" and "negative filtering," which phrases do not even appear in the independent claims. BT's cited cases are irrelevant because PAN agrees that, for data to be "post-filtering residue," it must go through filtering, and during that filtering it is neither selected nor discarded. This does not mean, however, that the filtering must include both a positive filter and a negative filter. As demonstrated by the hypotheticals, data can be "neither selected nor discarded" without undergoing both positive and negative filtering.

[2] "Pl. Op. Brief" refers to Plaintiff's Opening Claim Construction Brief.

b) The Dependent Claims Demonstrate That Positive Filtering And Negative Filtering Are Not Both Required.

BT argues that "PAN's proposed construction is also inconsistent with the dependent claims." Pl. Op. Brief at 11. BT's argument is without merit. The dependent claims do ***not*** impose an "additional round of positive *or* negative filtering." Pl. Op. Brief at 11. On the contrary, the dependent claims support PAN's proposed construction. The independent claims require "analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." '237 Patent at Claims 1, 18, 26. Dependent claims 2 and 27 narrow the independent claims by requiring that the "analysis" be a "multi-stage analysis."[3] Dependent claims 3 and 28, further narrow claims 2 and 27, by requiring that "said multi-stage analysis includes performing a discrimination analysis of said status data."[4] Dependent claims 4 and 29, further narrow claims 3 and 28, by requiring that "the discrimination analysis includes positive filtering." And dependent claims 5 and 30, further narrow claims 3 and 28, to require "the discrimination analysis includes negative filtering." Accordingly, BT's proposed construction cannot be correct, because it renders dependent claims 4, 5, 29, and 30 moot. That is, if the independent claim already requires ***both*** positive and negative

[3] Dependent claims 2 and 27 do not add anything to the independent claims, which already recite that the identifying step includes a multi-stage analysis, *i.e.*, "wherein the analysis includes filtering followed by an analysis of post-filtering residue." The specification confirms that filtering is a type of analysis. '237 Patent at 8:57-59.

[4] Dependent claims 3 and 28 do not add anything to the claims from which they depend. The independent claims already recite multi-stage analysis (filtering and post-residue analysis), and the specification confirms that filtering and post-residue analysis are examples of data discrimination analyses. '237 Patent at 8:57-59.

filtering, the addition of positive filtering and negative filtering in claims 4, 5, 29, and 30 does not further narrow the independent claims.

In contrast to BT's position, PAN's position gives meaning to dependent claims 4, 5, 29 and 30. *Merck & Co., Inc. v. Teva Pharm. USA, Inc.*, 395 F.3d 1364, 1372 (Fed. Cir. 2005) (holding that "claim construction that gives meaning to all the terms of the claim is preferred over one that does not do so."); *see also Sprint Spectrum L.P. v. Gen. Access Sols., Ltd.*, 812 Fed. App'x 999, 1003 (Fed. Cir. 2020). That is, dependent claims 4 and 29 require positive filtering (which is only optional in the independent claims) and dependent claims 5 and 30 required negative filtering (which is only optional in the independent claims).

c) The Specification Describes A Probe With Only Negative Filters, Only Positive Filters, Or Both

PAN's proposed construction is also supported by embodiments in the specification that contemplate that the data may pass through only a positive filter or only a negative filter. For example, the "Detailed Description of the Invention" states:

> Probe/sentry system 2000 collects and filters (**positively and/or negatively**) or otherwise analyzes the constantly updated status data it receives from sensors, using a set of rules and/or filters looking for evidence or 'footprints' of unauthorized intrusions.

'237 Patent at 5:19-23. The specification's use of "and/or" demonstrates, consistent with PAN's proposed construction, that "filtering" includes either positive filtering, negative filtering, or both. But BT's construction improperly excludes this embodiment. *GE Lighting Sols., LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1311 (Fed. Cir. 2014) ("[W]here claims can reasonably [be] interpreted to include a specific embodiment, it is incorrect to construe the claims to exclude that embodiment, absent probative evidence on the contrary."). Moreover, numerous other embodiments describe the claimed filtering without requiring both positive and negative filtering. '237 Patent at Abstract

("The probe filters and analyzes the collected data to identify potentially security-related events happening on the network."), 1:49-54 ("In an exemplary implementation . . . using a probe or 'sentry' system, collects status data from monitored components, filters or otherwise analyzes the collected data . . . "), 3:10-13 ("Once the probe/sentry system collects the data, it then filters or otherwise analyzes such data and then transmits noteworthy information . . . ").

BT contends that "the term 'residue' is explicitly ***defined*** in the specification" at column 8, lines 55-59—"Data neither discarded by negative filtering subsystem 2020 nor selected out as interesting by positive filtering subsystem 2030 form 'residue,' which is sent to anomaly engine 2050 for further analysis." Pl. Op. Brief at 5. But BT fails to meet the high threshold to establish that it "acted as his own lexicographer" by "clearly express[ing] intent in the written description" to define terms and act with "reasonable clarity, deliberateness, and precision." *Merck & Co., Inc.*, 395 F.3d at 1370; *see also In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). There is no clearly expressed intent in the specification to support BT's construction requiring both positive and negative filtering.

The sole passage from the specification that BT cites does not meet the threshold for lexicography. The cited passage is part of a paragraph relating to Figure 2, which is plainly described as "an ***exemplary*** embodiment." '237 Patent at 8:35-59. As explained above, the specification describes other embodiments that contemplate either positive filtering and/or negative filtering. *Id.* at 5:19-23 ("Probe/sentry system 2000 collects and filters (***positively and/or negatively***) or otherwise analyzes the constantly updated status data…"). Accordingly, BT's cited passage does not clearly express an intent to limit the claims as BT proposes, and reading it as such would amount to improperly "importing limitations from the specification into the claims." *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 905 (Fed. Cir. 2004); *see also Cont'l Cirs.*

LLC v. Intel Corp., 915 F.3d 788, 798 (Fed. Cir. 2019); *Comark Commc'n Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998); *E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 849 F.2d 1430, 1433 (Fed. Cir. 1988).

Indeed, the patentee represented to the Patent Office that the "term 'post-filtering residue' is clearly defined, ***in the claim language itself***, as data that is neither discarded nor selected by filtering." '237 File History at JA-0000121. BT cannot now contend that this term is "explicitly defined in the specification" by reference to an exemplary embodiment that includes both a positive filtering subsystem and a negative filtering subsystem. The claim language requires only that the residue result from "an analysis including filtering"—it does not specify or require both a positive filtering subsystem and a negative filtering subsystem. The patentee could have drafted the independent claims to recite that "the analysis includes ***positive and negative filtering*** followed by an analysis of post-filtering residue"—but they did not. Instead, positive and negative filtering are recited in the dependent claims.

BT further contends that ***both*** positive and negative filtering are required by "the sole embodiment describe in the specification." Pl. Op. Brief at 7. That is simply incorrect. BT ignores the additional embodiments described above that ***do not*** require both positive and negative filtering. '237 Patent at 5:19-23; *see also id.* at Abstract, 1:49-54, 3:10-12. And, the embodiment BT relies on is described as an "exemplary embodiment." *Id*. at 8:35-53. Moreover, even if BT's embodiment was the "sole embodiment" as it contends, as explained above, it "is improper to read limitations from a preferred embodiment described in the specification—even if it is the only embodiment—into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited." *Liebel-Flarsheim.*, 358 F.3d at 913.

d) The Prosecution History Does Not Require The Claimed Filtering To Include Both Positive Filtering And Negative Filtering

BT contends that the prosecution history supports its construction, but BT mischaracterizes a variety of disjointed quotes without context. For example, BT points to the applicant's argument when distinguishing the prior art because "no mention is made of analyzing data that was not discarded and that was not also [*sic*] selected by the filtering process." Pl. Op. Brief at 9 (citing '237 File History at JA-0000096 (Applicant's Arguments and Remarks at 11 (Apr. 13, 2005))). BT, however, omits the next line, which illuminates the true focus of the applicant's argument: "Any analysis performed by [the prior art reference] is clearly done on alerts that were **selected** by the filtering process." *Id.* Thus, the key distinction that the applicant made to differentiate the prior art reference from the claims was that the "post-filtering residue" must ***not*** have been selected or discarded by filtering. In contrast, the prior art reference analyzed data that was selected (*i.e.*, matched a positive filter). The applicant's argument did not require both positive filtering and negative filtering.

Similarly, BT mischaracterizes a separate argument within the '237 File History from nearly a year later where the applicant distinguishes prior art that "discloses data that is selected by filtering" and data that "is discarded in the filtering process." *See* '237 File History at JA-0000122-23 (Applicant's Arguments and Remarks at 9-10 (Feb. 7, 2006)). Again, the crux of the applicant's distinction is whether the prior art had "post-filtering residue" – data neither selected nor discarded. The applicant argued that prior art did not have post-filtering residue as it only analyzed data that ***was*** selected or discarded. *Id.* Thus, the '237 File History and the distinctions that applicant relies upon further demonstrate that there is no requirement to ***both*** negatively filter and positively filter data, as proposed by PAN. Because PAN's construction is

consistent with the prosecution history, the plain language of the claims, and the specification, the Court should adopt PAN's construction.

e) The Plain And Ordinary Meaning Of "post-filtering residue," Is "data that does not match any filter (*i.e.*, discarding (negative) filter or selecting (positive) filter)"

The plain and ordinary meaning of "post-filtering residue" that should be adopted is "data that does not match any filter (*i.e.*, discarding (negative) filter and/or selecting (positive) filter)." This plain and ordinary meaning is consistent with the claim language and specification, and eliminates any confusion from the inconsistent usage of these terms in BT's infringement contentions. *See supra* Section II.A.1 (describing BT's inconsistent usage of "positive filter" as one that discards and "negative filter" as one that selects").

The language of the independent claims provides that "post-filtering residue is data neither discarded nor selected by filtering." '237 Patent at Claims 1, 18, 26. PAN's proposed construction of the plain and ordinary meaning simply mirrors the claim language. *See E.I. Du Pont De Nemours & Co. v. Unifrax I, LLC*, 921 F.3d 1060, 1079 (Fed. Cir. 2019) ("[c]laims mean precisely what they say."); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) ("[W]e look to the words of the claims themselves...to define the scope of the patented invention.") (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). The claimed language "data neither discarded nor selected" is equivalent to "data that does not match any filter (*i.e.*, discarding (negative) filter and/or selecting (positive) filter)." And as explained above, "filtering" does not require ***both*** positive and negative filtering. Further, the specification's description of the terms "positive filtering" and "negative filtering" also corresponds to the plain and ordinary meaning of "post-filtering residue." '237 Patent at 8:35-59 (describing "negative

filtering . . . which discards" and "positive filtering . . . which selects."). Thus, PAN's proposed construction of the plain and ordinary meaning is consistent with the claims and specification.

3. Term Nos. 2-3: "analysis includes filtering" / "filtering"

Term	Claim Nos.	BT's Proposed Construction	PAN's Proposed Construction
analysis includes filtering	Claims 1, 18, 26	Analysis includes positive filtering to select interesting information and negative filtering to discard uninteresting information	N/A[5]
filtering	Claims 1, 18, 26	N/A	Discarding data that matches a filter rule (negative filtering) and/or selecting data that matches a filter rule (positive filtering)

Term Nos. 2 and 3 present the same dispute as Term No. 1 regarding whether "filtering" requires both positive and negative filtering. For the same reasons described above, the Court should find that these terms do not require both positive and negative filtering. Additionally, as explained below, PAN's proposed constructions for Term Nos. 2 and 3 provide a necessary clarification and BT's arguments to the contrary are unavailing.

PAN's construction is consistent with the plain language of the claims and adds clarity to the meaning of "filtering." "Filtering" involves either discarding or selecting data when that data matches a filter criteria. As described above, this clarification is necessary because BT's infringement contentions confuse and conflate "selecting" with "matching." The specification states that "selecting" or forwarding is an action taken by a filter on "interesting information" after

[5] The parties have proposed different terms for construction. BT proposes construing "analysis including filtering" and PAN proposes construing "filtering." Thus, "N/A" corresponds to the terms for which each party is not proposing a construction.

incoming data matches a criterion of the filter. '237 Patent at 8:45-50; Claims 1, 18, 26. PAN's proposed construction adds this necessary clarification from the specification to the meaning of "filtering."

To the extent BT complains that PAN's construction "injects the phrase 'filter rule,'" PAN is amenable to substituting an alternative such as "filter criterion"—*i.e.*, discarding data that matches a filter criterion and/or selecting data that matches a filter criterion. *See* Pl. Op. Brief at 8. BT does not dispute, and cannot dispute, that "filtering" involves comparing incoming data to a rule or criterion, and then taking a specified action if the data matches the filter rule/criterion. Ex. 1 at ¶¶ 26-31.

BT's construction requires "positive filtering to select ***interesting information***" and "negative filtering to discard ***uninteresting information***," but does not inform the jury what constitutes "interesting information" and "uninteresting information." Thus, BT's construction will not help a jury understand the "filtering" terms because it provides no guidance on how filters actually function in the claimed invention. *See Power-One, Inc. v. Artesyn Techs., Inc.*, 599 F.3d 1343, 1348 (Fed. Cir. 2010) ("The terms, as construed by the court, must 'ensure that the jury fully understands the court's claim construction rulings and what the patentee covered by the claims.'"); *see also Funai Elec. Co. v. Daewoo Elecs. Corp.*, 616 F.3d 1357, 1366 (Fed. Cir. 2010) ("The criterion is whether the explanation aids the court and the jury in understanding the term as it is used in the claimed invention."). The addition of such subjective terms such as "interesting" and "uninteresting" to a construction does nothing but adds ambiguity and uncertainty as to how the filters are selecting and discarding information. As such, the Court should not adopt BT's unhelpful construction.

B. Term No. 6: "security-related events"

Term	Claim Nos.	BT's Proposed Construction	PAN's Proposed Construction
security-related events[6]	Claims 1, 18, 24, 26	An attack or intrusion against the computer network	Attacks or intrusions against the computer network

BT is correct that both parties seem to generally agree as to the meaning of this term. It is PAN's position, however, that this term is better understood within the context of the broader limitation that includes this term—*see* Term No. 7. *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 791 (Fed. Cir. 2021) ("it is not always appropriate to break down a phrase and give it an interpretation that is merely the sum of its parts."); s*ee* '237 Patent at Claims 1, 18, 26 ("analyzing status data to identify potentially security-related events represented in the status data"); *see also id.* at Abstract ("The probe filters and analyzes the collected data to identify potentially security-related events happening on the network. Identified events are transmitted to a human analyst for problem resolution.").

Notably, for Term Nos. 2 and 3, BT demands construing "filtering" with the two preceding words, "analysis includes filtering"; and BT utilized over a page of its opening brief to argue the importance of construing "the entirety of the relevant claim limitations" and that failure to do so is "legally improper and unnecessarily confusing." *Id.* In that same vein, PAN's position is that, whatever the construction of "security related-events," the claim limitation as a whole requires identification of ***potentially*** security-related events and not identification of actual security-related events. *Infra* Term No. 7.

[6] To avoid any confusion, PAN notes that there are no terms to construe for Term Nos. 4 and 5.

Further, PAN proposes the plural version of BT's proposed construction to align with the rules of grammar.

C. Term No. 7: "identify potentially security-related events represented in the status data"

Term	Claim Nos.	BT's Proposed Construction	PAN's Proposed Construction
identify potentially security-related events represented in the status data	Claims 1, 18, 26	Determine what status data is believed to be footprints (evidence) of "security-related events"	No construction required. Alternatively, "identify potential attacks or intrusions against the computer network represented in the status data"

PAN does not believe a construction is necessary for this term because the claim language is clear—"analyzing status data to identify potentially security-related events represented in the status data." '237 Patent at Claims 1, 18, 26. The Court should reject BT's construction as it would confuse the jury and erases the import of the word "potentially."

First, BT contends that "[t]he term 'identify potentially security-related events represented in the status data' requires an ***actual determination*** as to what status data is ***believed to be footprints*** of security-related events." Pl. Op. Brief at 15. BT's position is nonsensical. It requires an "actual determination," yet it is a "belie[f]" based on "footprints." This construction would be confusing for the jury and should be rejected.

Second, BT's construction is an improper attempt to erase the word "potentially." BT states in its opening brief that "identify[ing] potentially security-related events requires more than merely determining that something *could* contain a security-related event," and that "being uncertain about whether a piece of data is or is not a security-related event is not the same as 'identify[ing] a potentially security-related event.'" Pl. Op. Brief at 17. But that uncertainty is all that is claimed. BT would erase any import to the term "potentially."

The claims require that the "potentially security-related events" are identified by an analysis that includes "filtering followed by an analysis of post-filtering residue." '237 Patent at Claims 1, 18, 26. Any data that is not discarded or selected by that filtering is "post-filtering residue." *Id.* The crux of the issue here is that post-filtering residue is inherently ***not known*** to the system because it did not match a filtering criterion. The probe merely "analyzes the collected data for activity ***possibly*** implicating security concerns." '237 Patent at 1:54-55. Indeed, the next claimed step is "transmitting information about said identified events to an analyst." '237 Patent at Claims 1, 18, 26. The analyst, not the probe, makes the actual determination whether there is a security-related event. "Once a ***possible*** attack or intrusion . . . is detected, its characteristics and particulars may then be examined and analyzed by trained security analysts . . . to further understand the incident and eliminate false positives." *Id.* at 2:3-8. There would not be a need to send data along to the security analyst if the probe was capable of making a determination on its own.

D. Terms No. 8 and 9: "feedback . . . based on empirically-derived information" / "empirically-derived information reflecting operation of said security monitoring system"

Term	Claim Nos.	BT's Proposed Construction	PAN's Proposed Construction
feedback . . . based on empirically-derived information	Claims 1, 18, 26	The information that is received was derived from an empirical analysis of the information previously transmitted	Indefinite
empirically-derived information reflecting operation of said security monitoring system	Claims 1, 18, 26	Not indefinite	Indefinite

PAN contends that the entire limitation "receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system" is indefinite. As such, PAN addresses both Term Nos. 8 and 9 together.

Terms No. 8 and 9 are indefinite because the intrinsic evidence fails to provide an objective boundary for the scope of the "empirically-derived information reflecting operation of said security monitoring system." Specifically, the claim language, specification, and prosecution history fail to inform a POSA with reasonable certainty what is the "information reflecting operation of said security monitoring system" that is being "empirically-derived." Ex. 1 at ¶¶ 32-41.

BT does not brief the issue of indefiniteness and incorrectly states that "[t]he parties agreed that terms which Defendant has identified as indefinite do not need to be briefed and will be addressed at the appropriate time." Pl. Op. Brief at 20. BT mischaracterizes the parties' agreement. The parties agreed to reserve briefing on indefiniteness as to ***certain terms*** identified in Section III of the Joint Claim Construction Chart. But the parties expressly agreed that indefiniteness of Term Nos. 8 and 9 should be addressed during claim construction. D.I. 119 at 16-19, 23-25. Instead of addressing indefiniteness, BT improperly attempts to rewrite the claim limitation to address the ambiguity. Therefore, the Court should reject BT's proposed construction and find that the claims are indefinite.

1. The Intrinsic Evidence Does Not Provide Reasonable Certainty And Instead Injects Further Ambiguity

Nothing in the claim language, specification, or prosecution informs what is the "information reflecting operation of said security monitoring system" that is being "empirically-derived." Ex. 1 at ¶¶ 33-41. In fact, while contemporaneous dictionaries provide some insight by defining "empirically" to mean "originating in or based on observation or experience," *id.* at ¶ 33

(citing Merriam-Webster Collegiate Dictionary's definition of "empirically"), the intrinsic evidence injects further ambiguity.

First, the claim language provides that the probe "transmit[s] information about said identified events to an analyst," and then presumably the analyst provides "feedback [to] the probe based on empirically-derived information reflecting operation of said security monitoring system." '237 Patent at Claims 1, 18, 26. A POSA would not have understood from the claims as to how the information transmitted to the analyst is used, if at all, to produce the feedback subsequently received by the probe. Ex. 1 at ¶ 34. While the claimed feedback is "based on empirically-derived information reflecting operation of said security monitoring system," there is no identified connection between the empirically-derived information and the information transmitted to the analyst. *Id.* Rather, there are important missing steps between "information about said identified events" and "empirically-derived information." *Id.*

Second, the specification fails to provide any guidance regarding those missing steps. Specifically, the specification provides no explanation of what "empirically-derived" means in relation to the claimed "information reflecting operation of said security monitoring system." *Id.* at ¶ 35. Rather, it provides that an "analyst may follow a predetermined escalation procedure in the event he or she is unable to resolve the problem without assistance from others." *Id.* (citing '237 Patent at Abstract). The specification further provides that "security analysts can draw upon information and knowledge contained in a variety of databases, including but not limited to security intelligence databases containing information about the characteristics of various hacker techniques and tools and known vulnerabilities in various operating systems and commercial software products and hardware devices." *Id.* (citing '237 Patent at 2:9-15). A POSA would not have understood as to what in the specification the claim language is referring to because the

specification describes that the analyst is considering so much information. Ex. 1 at ¶¶ 35-36. A POSA would thus not be able to determine the boundaries of the claimed "empirically-derived information." *Id.* Moreover, a POSA would have understood that some of this information does not even "reflect[the] operation of said security monitoring system," but the descriptions of predetermined escalation procedure and databases do not provide any boundaries for what does. *Id.* at ¶ 36. Therefore, the specification does not inform a POSA as to what "empirically-derived" means in relation to the claimed "information reflecting operation of said security monitoring system." *Id.* at ¶¶ 35-36.

Finally, this issue was not addressed during the prosecution. Accordingly, it is not reasonably certain from the intrinsic evidence regarding what information is being "empirically-derived."

2. BT's Proposed Construction Attempts to Rewrite The Claim Language And Creates Further Confusion

a) The Court Should Reject BT's Attempt to Rewrite the Claims

BT recognizes that the terms as written lack reasonable certainty and attempts to resolve that uncertainty by rewriting the claim in its proposed construction. Specifically, BT attempts to resolve ambiguity by substituting the word "feedback" with "the information that is received." Quite differently from the claim language, BT's construction requires that the feedback is "derived from an empirical analysis of the information previously transmitted." *Id.* at ¶¶ 42-43. The existing claim language states only that feedback is based on empirically-derived information, without providing clarity as to what is being empirically analyzed. *Id.* This is apparent when comparing the existing claim language with Plaintiff's new claim language via its proposed construction:

> **Claim Language:** "receiving feedback…based on empirically-derived information reflecting operation of said security monitoring system."
>
> **Plaintiff's Proposed New Claim Language**: "the information [*i.e.*, feedback] that is received was derived from an empirical analysis of the information previously transmitted."

Id. at ¶ 43.

Moreover, BT's construction completely eliminates the language "reflecting operation of said security monitoring system." Therefore, with regard to Term No. 9 specifically, BT cannot argue that "reflecting operation of said security monitoring" provides any certainty regarding the scope of "empirically-derived information" when its proposed construction writes that aspect out of the claim. A POSA would not know with reasonable certainty the scope of that language that Plaintiff is attempting to remove from the claim via its proposed construction. *Id.* at ¶¶ 42-44. Therefore, the Court should reject BT's attempt to fix the ambiguity post-hoc and find this limitation indefinite. *Chef America, Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1374 (Fed. Cir. 2004) ("courts may not redraft claims, whether to make them operable or to sustain their validity.").

b) BT's Proposed Construction Creates Ambiguity as to Whether a Human Analyst Conducts Analysis

A POSA, after reading the claims and specification, would understand that the very nature of the invention is to incorporate a human analyst in the loop, and in doing so not to rely solely on automated defenses. Ex. 1 at ¶¶ 38-39 (explaining that prior claim limitation provides "transmitting information about said identified events ***to an analyst*** associated with said security monitoring system."); *see also id.* (citing '237 Patent at Abstract; Figs. 5, 6, 7, 8; 1:33-42, 1:49-59, 2:3-20, 2:35-42, 2:59-61, 3:39-47, 7:31-43, 9:13-15, 9:52-56, 10:10-18, 10:41-67, 11:1-3, 11:13-52). But BT's proposed construction and infringement contentions show that BT is

attempting to improperly broaden the claims to cover fully automated activity that does not involve any feedback from a human analyst. Ex. 7 at 56-71 (BT asserting in infringement contentions that a fully automated feedback (that does not involve a human analyst) meets the claim limitations). Indeed, "analyst" is never mentioned in BT's argument for Term Nos. 8 or 9. Pl. Op. Brief at 18-20. In fact, "analyst" is only mentioned once in BT's preliminary statement and quoted once more when arguing Term No. 7. *Id.* at 1, 16. Rather, BT contends that the feedback is from the SOC and offers as evidence that:

> [T]he '237 Patent describes ***feedback 'from the SOC*** designed to mitigate or terminate various attacks.' '237 Patent, 9:22-30. In response to detecting 'someone repeatedly trying to log in to the customer's network,' the ***SOC performs an empirical analysis*** and determines "to not allow a certain IP address to access the customer's network for the next 10 minutes." *Id.*

Id. at 19-20. As with the other terms above, BT extrapolates this evidence by omitting significant portions of the specification that reveal that the SOC does not provide feedback. In fact, the specification provides that "requests ***originating*** from the SOC [are] designed to mitigate or terminate various attacks." '237 Patent at 9:29-30. BT is undoubtedly trying to hide that the claims incorporate a human analyst.

BT's position in the IPRs creates further ambiguity. Specifically, BT asserts that feedback "based on empirically-derived information" does not include feedback that is based on subjective views. Ex. 1 at ¶ 40 (citing JA-0000662 (BT's Preliminary Response, IPR2019-01324) ("subjective beliefs … are not objectively verifiable … [and] is therefore based on the exact opposite of 'empirically-derived information.' In fact, the subjective nature … precludes the empirically-driven approach disclosed by [the '237 Patent]."); JA-0000665 (BT's Preliminary Response, IPR2019-01324) ("empirically-derived information, which is fundamentally unlike determining whether something is subjectively objectionable."); JA-0000694 (Wenke Lee's

Declaration, IPR2019-01324) ("Subjective preferences are not empirically-derived information, because they are not objectively verifiable—varying from person to person.")). The specification does not disclose an analyst (or anything else) performing an empirical analysis of information that was previously transmitted (from the probe to the analyst). *Id.* On the other hand, the specification describes the analyst's process as "match[ing] the observed symptoms of the attack to a known vulnerability," *id.* (citing '237 Patent at 10:61-62), or as BT provided, "confirm[ing] whether they are actual security events," *id.* (citing JA-0000616-17 (BT's preliminary response, IPR2019-01324)). In the manner described by the '237 Patent, this analysis would necessarily involve the subjective views of the analyst. *Id.* Therefore, under BT's position in the IPRs, the human's analysis would not constitute empirical analysis.

* * *

For the foregoing reasons, PAN respectfully requests that the Court conclude that Term Nos. 8 and 9 be held indefinite for failing to provide an objective boundary for the scope of the "empirically-derived information reflecting operation of said security monitoring system."

April 24, 2024

Respectfully submitted,

FARNAN LLP

/s/ Brian E. Farnan

Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
919 North Market St., 12th Floor
Wilmington, DE 19801
Tel: (302) 777-0300
Fax: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Adrian C. Percer (admitted *pro hac vice*)
Gregg T. Stephenson (admitted *pro hac vice*)
Weil, Gotshal & Manges LLP
201 Redwood Shores Parkway
Redwood Shores, CA 94065
Telephone: (650) 802-3000
adrian.percer@weil.com
gregg.stephenson@weil.com

Anish R. Desai (admitted *pro hac vice*)
Ian Moore (admitted *pro hac vice*)
Tom Yu (admitted *pro hac vice*)
Weil, Gotshal & Manges LLP
767 Fifth Avenue
New York, NY 10153
Telephone: (212) 310-8000
anish.desai@weil.com
ian.moore@weil.com
tom.yu@weil.com

Priyata Y. Patel (admitted *pro hac vice*)
Weil, Gotshal & Manges LLP
2001 M Street, NW Suite #600
Washington, D.C. 20036
Telephone: (202) 682-7000
priyata.patel@weil.com

Attorneys for Defendant Palo Alto Networks, Inc.

EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BRITISH TELECOMMUNICATIONS PLC and BT AMERICAS, INC., *Plaintiffs*, v. PALO ALTO NETWORKS, INC. *Defendant*.	C.A. No. 22-01538-CJB

DECLARATION OF DR. JOHN VILLASENOR IN SUPPORT OF DEFENDANT PALO ALTO NETWORK, INC.'S ANSWERING CLAIM CONSTRUCTION BRIEF

1. My name is Dr. John Villasenor, Ph.D. and I have been retained as an expert witness on behalf of Palo Alto Networks, Inc. ("PAN") to provide expert opinions on certain claim construction issues related to U.S. Patent No. 7,159,237 ("the '237 Patent).

I. EXPERIENCE AND QUALIFICATIONS

2. I have either trained or worked in computer algorithms, devices, networks, and architectures for approximately four decades. My work addresses innovative, high-performance communications, networking, media processing, and computing technologies and their broader implications.

3. I received a B.S. in electrical engineering from the University of Virginia in 1985, a M.S. in electrical engineering from Stanford University in 1986, and a Ph.D. in electrical engineering from Stanford University in 1989. Between 1990 and 1992, I worked for the Jet Propulsion Laboratory in Pasadena, CA, where I developed techniques for imaging and mapping the Earth from space.

4. Since 1992, I have been on the faculty of the Electrical Engineering Department of the University of California, Los Angeles ("UCLA"). Between 1992 and 1996, I was an Assistant Professor; between 1996 and 1998, an Associate Professor; and since 1998, I have been a full Professor. For several years starting in the late 1990s, I served as the Vice Chair of the Electrical Engineering Department at UCLA. In addition to my faculty appointment in the UCLA Samueli School of Engineering, I hold faculty appointments (and have taught classes) in the UCLA School of Law, the Department of Public Policy within the UCLA Luskin School of Public Affairs, and the UCLA Anderson School of Management. I am also the founder and faculty co-director of the UCLA Institute for Technology, Law, and Policy.

5. In the UCLA Samueli School of Engineering, I have taught courses addressing digital signal processing, communications, and networking (including consideration of the associated security and management challenges), systems, algorithms, devices, and networks. In addition to my teaching, I have performed extensive research at UCLA over the past several decades on multiple aspects of: digital devices, systems, and networks, including device and network security, device design, integration and use of devices within the context of larger networks; acquisition, processing, and communications of data; communications and protocols used to convey information among networked devices; approaches to monitor the activity on and ensure the security of networks, optimization to achieve goals including low power consumption and high speed; and mapping of algorithms onto hardware. My work has considered hardware and software, and has included consideration of factors such as configuration and control of devices, network architecture, protocols, security, the interaction among devices, as well as between humans and devices, and artificial intelligence.

6. An important aspect of my research, which I have also incorporated into my teaching, involves ensuring the reliability, integrity, and security of information and networks. This includes protocols and other aspects of network design that can maximize performance and efficiency, approaches to assess the trustworthiness of information sources, measures to ensure information is not altered or captured without authorization, and approaches to model increasingly complex networks to better identify their behavior and vulnerabilities. My work in cybersecurity has led, among other things, to my selection to lead a project funded by the Department of Homeland Security aimed at protecting U.S. critical infrastructure, to technical advances relating to improving the performance, reliability, and security of the computing devices and networks that are so critical in today's society, and to contributions relating to U.S. policy aimed at helping to ensure the integrity and security of defense-critical devices and networks.

7. My UCLA research has been funded by organizations including DARPA, the U.S. Office of Naval Research, the National Science Foundation, and multiple companies.

8. I am an inventor on approximately 20 issued U.S. patents in areas including information processing, data compression, communications, and cybersecurity. I have published over 175 articles in peer-reviewed journals and academic conference proceedings. I have also been asked on multiple occasions to provide congressional testimony on technology topics.

9. In addition to my work at UCLA, I am a nonresident senior fellow at the Brookings Institution in Washington, D.C. Through Brookings I have examined a wide range of topics at the technology/policy intersection including AI, cybersecurity, wireless mobile devices and systems, and artificial intelligence. In addition to publishing in traditional academic venues such as engineering journals, engineering conference proceedings, and law reviews, I have published

papers through the Brookings Institution, and articles and commentary in broader-interest venues including *Billboard*, the *Chronicle of Higher Education*, *Fast Company*, *Forbes*, the *Los Angeles Times*, the *New York Times*, *Scientific American Slate*, and the *Washington Post*.

10. I have also been a senior fellow at the Hoover Institution at Stanford and an affiliate of the Center for International Security and Cooperation ("CISAC") at Stanford. In relation to those affiliations, I have led a research project funded by the U.S. Department of Homeland Security aimed at improving cybersecurity in U.S. critical infrastructure. I am also a member of the Council on Foreign Relations.

11. I have several decades of experience in early-stage technology venture capital in the San Francisco Bay Area. In that capacity, I have met with a large number of startup companies seeking venture financing spanning a wide range of technology areas. Among other things, I have helped to evaluate the proposed technology, the competitive landscape, the market landscape including opportunities and risk, the nature and extent of customer demand, the strength of the team, and the company's IP strategy and position. I have also served as a consultant to many companies over the years that I have been on the faculty at UCLA.

12. Further details of my background and experience are provided in my curriculum vitae, which is attached as Appendix A.

II. MATERIALS REVIEWED

13. I have been asked by counsel for defendants to render opinions on various issues in this case relating to the inventions claimed in the '237 Patent. In reaching the conclusions stated in this Declaration, I have relied upon my over 30 years of experience and knowledge in the field of cybersecurity. I have also considered the materials listed in Exhibit 2 of my Expert Declaration,

including the ’237 Patent, the prosecution histories for the ’237 Patent and the related U.S. Patent No. 7,895,641 (“the ’641 Patent”), the parties’ Joint Claim Construction Chart filed on February 23, 2024, Plaintiff’s Opening Claim Construction Brief served on March 25, 2024, and any other documents cited herein.

III. RELEVANT LEGAL STANDARDS

A. Person of Ordinary Skill in the Art

14. I am informed that patent claims should be understood from the perspective of a person of ordinary skill in the relevant art to which the patent is related and based on the understanding of that skilled person at the time the application was filed.

15. A person of ordinary skill in the art (“POSA”) at the time of the ’237 Patent would have had a B.S. degree in Computer Science, Computer Engineering, or an equivalent field, as well as at least 2-3 years of academic or industry experience in the design, analysis, and monitoring of computer networks, including issues of network security and network management, or comparable industry experience.

16. As reflected in my qualifications set forth above, I have substantial experience and expertise with computer algorithms, devices, networks, and architectures, including the related network security and management issues. I am at least a person of ordinary skill in the art and was also at least a person of ordinary skill in the art in 2001, when application leading to the ’237 Patent was filed.

B. Claim Construction and Indefiniteness

17. In formulating my opinions, counsel has provided me with an understanding of certain principles of U.S. patent law that govern determinations of claim construction and patent

validity. The discussion of legal principles set forth below is not exhaustive, and is intended to provide context for the opinions that I provide.

18. I understand that for claim construction purposes, the Court will look to the meaning that would have been ascribed to the claim terms or understood by a person having ordinary skill in the art ("POSA") at the time of the invention. I understand that a POSA is a hypothetical person who is presumed to have known and reviewed all of the relevant art at the time of the invention. Factors that may be considered in determining the level of ordinary skill in the art may include: (a) the types of problems encountered in the art; (b) prior art solutions to those problems; (c) the rapidity with which innovations are made; (d) the sophistication of the technology; and (e) the educational and/or experience level of active workers in the field.

19. I understand that to determine how the skilled person would have understood claim language, the Court first looks to the "intrinsic evidence"—the plain meaning of the words of the claims themselves, the patent specification, and the prosecution history of the patent, including any post-grant proceedings.

20. I understand that the Court may also consider "extrinsic evidence," including all evidence external to the patent and prosecution history, such as scientific articles and expert testimony concerning relevant scientific principles, the meanings of technical terms, and the state of the art. I understand that extrinsic evidence can be helpful to assist the Court in understanding what a skilled person would have known at the time that the patent application was filed.

21. I have been informed that U.S. patent law requires that the claims of a patent must particularly point out and distinctly claim the subject matter of the invention, such that a POSA would understand the bounds of the claim when read in light of the specification and the

prosecution history. I understand that the purpose of this requirement is to provide the public with clear notice of what is claimed, thereby apprising the public of what is still open to them.

22. I have also been informed that a patent claim, viewed in light of the specification and prosecution history, must inform the POSA about the scope of the invention with reasonable certainty. Specifically, patent claims, when read in light of the specification and the prosecution history, must provide objective boundaries for those of skill in the art.

IV. BACKGROUND ON THE ART OF THE '237 PATENT

23. The '237 Patent, entitled "Method and system for dynamic network intrusion monitoring, detection and response," claims priority to an application filed on January 19, 2001. It is my understanding that, for purposes of my analysis, the meaning of the claim language should be evaluated by a POSA as it would have been understood as of January 19, 2001.

24. The '237 Patent has 42 claims. I have been informed that the parties agreed that Claim 18 (reproduced below) is the representative of all three independent claims of the '237 Patent:

> 18. A security monitoring system for a computer network, comprising:
>
> a) a plurality of sensors for monitoring components of said network;
>
> b) at least one secure operations center configured to receive and analyze potentially security-related event data from at least one probe; and
>
> c) at least one probe, wherein said probe is configured to
>
> (1) collect status data from at least one sensor monitoring at least one component of said network;
>
> (2) analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;

> (3) transmit information about said identified events to an analyst associated with said secure operations center;
>
> (4) receive feedback based on empirically-derived information reflecting operation of said security monitoring system; and
>
> (5) dynamically modify an analysis capability of said probe during operation thereof based on said received feedback.

'237 Patent at 36:38-63.

25. The '237 Patent relates to "network security and, more specifically, to methods and systems for dynamic network intrusion monitoring, detection and response." *Id.* at 1:7-9. In particular, the '237 Patent describes a security monitoring system comprising a probe that "filters and analyzes" collected data "to identify potentially-security related events happening on the network." *Id.* at Abstract. "Identified events are transmitted to a human analyst for problem resolution." *Id.*

A. Background on Filtering in Network Security

26. In the network security field, filtering was well-known in the art by January 19, 2001. A POSA would have understood "filtering" in this context to mean comparing data with a known criterion, and, if the data matches that criterion, then taking a specific action. *See* '237 Patent at 8:45-59; Ex. 4 at 3; Ex. 5 at 65; Ex. 6 at 754. The specific actions that a filter could take include discarding data (*i.e.* blocking) and selecting data (*i.e.* allowing). Filters that discard data are referred to as "negative filters" and filters that select data are referred to as "positive filters."

27. The '237 Patent describes positive and negative filtering exactly this way and acknowledges that they were "well-known to those skilled in the art":

> Once collated, the data is first filtered by **negative filtering subsystem 2020, which discards** uninteresting information, and then by **positive filtering subsystem 2030, which selects** possibly interesting information and forwards it to

> communications and resource coordinator 2060. Data neither discarded by negative filtering subsystem 2020 nor selected out as interesting by positive filtering subsystem 2030 form the "residue," which is sent to anomaly engine 2050 for further analysis. Anomaly engine 2050 determines what residue information may be worthy of additional analysis and sends such information to communications and resource coordinator 2060 for forwarding to the SOC. **Negative filtering, positive filtering, and residue analysis are examples of data discrimination analyses, other types of which are well-known to those skilled in the art.**

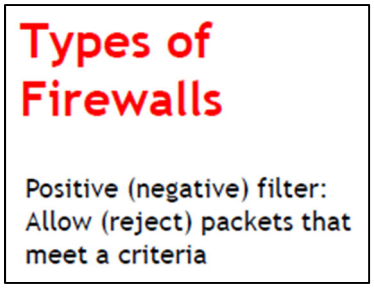
'237 Patent at 8:45-59 (emphasis added).

28. Indeed, that is how the prior art described negative and positive filtering. For example, Mr. Dan Strom's 2000 article entitled "The Packet Filter: A Basic Network Security Tool" describes well-known filtering technology. Ex. 4. A filter on a network "either blocks the datagram from passing or allows the datagram to pass." *Id.* at 1. The action taken by the filter is "based upon certain criteria defined to the packet filtering tool." *Id.* More specifically, a "filtering device compares the values of these fields to rules that have been defined, and based upon the values and the rules the packet is either passed or discarded." *Id.* at 2.

29. The usage of the terms "positive filter," which refers to a filter that selects data that matches a criterion, and "negative filter," which refers to a filter that discards data that matches a criterion, is consistent with the art at the time of the invention. As another example, a textbook entitled "Cryptography and Network Security: Principles and Practice" provides:

> A firewall may act as a packet filter. It can operate as **a positive filter, allowing** to pass only packets that meet specific criteria, or as a **negative filter, rejecting** any packet that meets certain criteria.

Ex. 2 at 22-5 (emphasis added). This is exactly how the terms are used throughout the industry and academia. In fact, "Cryptography and Network Security: Principles and Practice," has been used to teach network security at the university level. For example, a course on "Information Security" at the University of Kansas that uses this textbook teaches students with lecture slides that provide:



Ex. 3 at 6.

30. Additional examples demonstrate the well-known use of filters that compare data with known criteria and take a specific action, such as selecting (positive filtering) or discarding (negative filtering):

> Generally, the filtering rules are expressed as ***a table of conditions and actions*** that are applied in a certain order until a decision to route [*i.e.* ***select***] or drop [*i.e.* ***discard***] the packet is reached. When a particular packet meets all the conditions specified in a given row of the table, the action specified in that row (whether to route or drop the packet) is carried out[.]

Ex. 5 at 65 (emphasis added); *see also* Ex. 6 at 754 (defining filter as "[a] device or program that separates data or signals in accordance with specified criteria"). In my opinion, this usage of "positive filters" to select and "negative filters" to discard is consistent with a person of skill in the art's understanding and the common usage of these terms.

31. Further, such filters were widely available, including various commercially available filters from "Cisco, Bay, and Lucent." Ex. 4 at 1. Moreover, around the 2000 timeframe, "operating systems [could] be configured for packet filtering" and "[v]irtually all commercial firewalls support[ed] packet filtering." *Id.*

V. CLAIM CONSTRUCTION OPINIONS

32. I have been asked to provide my technical opinion on whether the definiteness requirement is satisfied for the claim limitation as exemplified in Claim 1 of the '237 Patent:

"receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system." I have reviewed the intrinsic evidence, and conclude this claim limitation is indefinite in light of the intrinsic evidence. The terms "empirically-derived" and "information reflecting operation of said security monitoring system" do not appear anywhere in the specification outside of the claims. These terms also were not discussed once during the prosecution of the '237 Patent. The claim language, specification, and prosecution history fail to inform one skilled in the art with reasonable certainty what is the "information reflecting operation of said security monitoring system" that is being "empirically-derived." Additionally, the intrinsic evidence is contradictory in such a way that it is ambiguous as to who or what is providing the feedback. Therefore, in my opinion, this claim limitation is indefinite.

A. The Claim Limitation is Indefinite Because the Intrinsic Record Does Not Provide Any Guidance on What Information Is Being "Empirically-Derived"

33. In my opinion, the '237 Patent's claim language and specification fail to inform a POSA on what information is being "empirically-derived." As described in the Merriam-Webster Dictionary, "empirically" means: "originating in or based on observation or experience." Ex. 8 at 379. This is consistent with my own understanding of "empirically."

34. The claim language does not provide any insight as to what information is being "empirically-derived." In fact, there are important steps unaddressed by the claim language—specifically, in between when the probe transmits information regarding the identified events to the analyst and when the probe receives feedback based on empirically-derived information reflecting operation of the security monitoring system. The '237 Patent claims a probe that "transmit[s] information about said identified events to an analyst." '237 Patent at 35:39-57. The '237 Patent then claims that the probe "receive[s] feedback … based on empirically-derived

information reflecting operation of said security monitoring system." *Id.* But the claim fails to provide any guidance as to how the information transmitted to the analyst is used, if at all, to produce the feedback that is received by the probe. While the claimed feedback is "based on empirically-derived information reflecting operation of said security monitoring system," there is no identified connection between the empirically-derived information and the information transmitted to the analyst.

35. The specification fails to provide any guidance regarding these missing steps. Specifically, the specification provides no explanation of what "empirically-derived" means in relation to the claimed "information reflecting operation of said security monitoring system." For example, when describing the analyst's role in this disclosed invention, the specification provides that the "analyst may follow a predetermined escalation procedure in the event he or she is unable to resolve the problem without assistance from others." *Id.* at Abstract. The specification further provides that "security analysts can draw upon information and knowledge contained in a variety of databases, including but not limited to security intelligence databases containing information about the characteristics of various hacker techniques and tools and known vulnerabilities in various operating systems and commercial software products and hardware devices." *Id.* at 2:9-15. The specification also provides that "analysts can be supplemented by a variety of knowledge databases containing detailed information helpful for investigating, evaluating and responding to incidents," wherein the "databases can contain information about, among other things, the characteristics of various network hardware and software products, known vulnerabilities of such products, the use and characteristics of various hacker tools, and known effective and ineffective responses to various kinds of attacks." *Id.* at 2:44-54. A plethora of information is provided to the

analyst; however, a POSA would not be able to determine the boundaries of the claimed "empirically-derived information."

36. The specification also fails to inform a POSA which of the information provided to the analyst "reflect[s the] operation of said security monitoring system." The descriptions of predetermined escalation procedure and databases do not provide any boundaries for what constitutes "information reflecting operation of said security monitoring system." By further example, the specification provides that when the analyst "determines … the symptoms, vulnerabilities and recommended solutions associated with the ticket," "the analyst … may use SOCRATES 6000 to match the observed symptoms of the attack to a known vulnerability. The analyst … can then search SOCRATES 6000 and its associated security intelligence and other databases for possible solutions." *Id.* at 10:56-65. Even though the specification describes the analyst using the "ticket," "SOCRATES," and "associated security intelligence and other databases," the specification does not inform a POSA as to the boundaries of what is being used by the analyst to produce feedback. This failure to inform renders the scope of Claim 1 unclear. Particularly, the specification does not help a POSA understand what "empirically-derived" means in relation to the claimed "information reflecting operation of said security monitoring system."

37. The prosecution history also does not speak to this issue. Thus, in my opinion, the intrinsic evidence provides no guidance on what information is being "empirically-derived."

B. Plaintiff's Proposed Construction Creates Ambiguity as to Whether a Human Analyst Conducts Analysis

38. A POSA would understand that the very nature of the invention is to incorporate a human analyst in the loop, and in doing so not rely solely on automated defenses. For example, the claim language in the prior limitation provides "transmitting information about said identified

events ***to an analyst*** associated with said security monitoring system." '237 Patent at 35:39-57 (emphasis added). The claims and the specification further inform a POSA that the analyst confirms the presence of unknown, potential intrusive activity for the system. *Id.* at Abstract; Figs. 5, 6, 7, 8; 1:33-42, 1:49-59, 2:3-20, 2:35-42, 2:59-61, 3:39-47, 7:31-43, 9:13-15, 9:52-56, 10:10-18, 10:41-67, 11:1-3, 11:13-52, 15:32-58.

39. However, Plaintiff's construction attempts to improperly broaden the claims to cover fully automated activity that does not involve feedback from a human analyst.

40. This is clear from reviewing the Plaintiff's Opening Claim Construction Brief. For example, Plaintiff selectively cites out of context in its Opening Claim Construction Brief that "the '237 Patent describes feedback 'from the SOC …'" and asserts that "the SOC performs an empirical analysis." Plaintiff's Opening Claim Construction Brief at 19-20. Actually, the '237 Patent provides that "requests ***originating*** from the SOC [are] designed to mitigate or terminate various attacks." '237 Patent at 9:22-30 (emphasis added). Plaintiff's assertion—that the SOC is performing an empirical analysis and providing the feedback—directly conflicts with the specification and obscures the fact that the claims incorporate a human analyst.

41. Plaintiff's statements during the IPRs creates further ambiguity. Plaintiff asserts that feedback "based on empirically-derived information" cannot encompass feedback that is based on subjective views. JA-0000662 (Plaintiff's Preliminary Response, IPR2019-01324) ("subjective beliefs … are not objectively verifiable … [and] is therefore based on the exact opposite of 'empirically-derived information.' In fact, the subjective nature … precludes the empirically-driven approach disclosed by [the '237 Patent]."); JA-0000665 (Plaintiff's Preliminary Response, IPR2019-01324) ("empirically-derived information, which is

fundamentally unlike determining whether something is subjectively objectionable."); JA-0000694 (Wenke Lee's Declaration, IPR2019-01324) ("Subjective preferences are not empirically-derived information, because they are not objectively verifiable—varying from person to person."). Again, Plaintiff's assertion—that "empirically-derived information" must be objectively verifiable—directly conflicts with the specification. The specification describes the analyst's process as "match[ing] the observed symptoms of the attack to a known vulnerability," '237 Patent at 10:59-62, or as Plaintiff provided, "confirm[ing] whether they are *actual* security events," JA-0000616-17 (Plaintiff's preliminary response, IPR2019-01324) (emphasis in original). A POSA would find that the analysis of data in the context of cybersecurity in the manner described by the '237 Patent would necessarily require the subjective views of the analyst. Therefore, under Plaintiff's position in the IPRs, the human's analysis would not constitute empirical analysis.

C. Plaintiff's Construction of "Feedback . . . Based On Empirically-Derived Information" Is Improper

42. I understand Plaintiff has proposed to construe the term "feedback … based on empirically-derived information" to mean "the information that is received was derived from an empirical analysis of the information previously transmitted."

43. It is my opinion that Plaintiff's proposed construction improperly re-writes the language to claim something entirely different. The claim language requires that the "feedback" is "based on empirically-derived information reflecting operation of said security monitoring system." However, in the context of this particular term, Plaintiff's construction attempts to resolve the above-mentioned ambiguity by substituting the word "feedback" with "the information that is received." Plaintiff's construction, quite differently from the claim language, requires that the

feedback is "derived from an empirical analysis of the information previously transmitted." This re-write of the claim completely alters the plain language in an attempt to specify what information is being empirically analyzed. But existing claim language includes no such limitation and instead only states that feedback is based on empirically-derived information without providing clarity as to what is being analyzed to obtain that empirically-derived information. This is apparent when comparing the existing claim language with Plaintiff's new claim language via its proposed construction:

> **Claim Language:** "receiving feedback … based on empirically-derived information reflecting operation of said security monitoring system."
>
> **Plaintiff's Proposed New Claim Language**: "the information [*i.e.*, feedback] that is received was derived from an empirical analysis of the information previously transmitted."

An additional concern with Plaintiff's construction is that it eliminates the language "reflecting operation of said security monitoring system." As I previously explained, a POSA would not know with reasonable certainty the scope of that language. Plaintiff's proposed construction simply removes that language from the claim.

VI. CONCLUSION

44. Accordingly, it is my opinion that the claim limitation "receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system" is indefinite.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Dated: April 23, 2024

/s/ John Villasenor
Dr. John Villasenor